次世代サイバー演習環境に向けて

太田 悟史[1]　安田 真悟[1]　湯村 翼[1]　高野 祐輝[1]

概要：
コンピュータやネットワークへのセキュリティ対策の重要性が高まるなかで, 高度化, 複雑化するサイバー攻撃についてはサイバー演習によるセキュリティ人材育成が急務となっている. 今後, より多くの人材の輩出が望まれているため, それに応じてより多くのサイバー演習の実施が必要となる. その一方で, サイバー演習環境の学習効果をより向上させるためには, リアリティと演習の振り返りへの対応が必要である. しかし, 高いリアリティは構築コストが高く, さらに, 振り返りの機能の分だけ運用コストが増大する. そこで本稿では, サイバー演習環境の構築効率の向上と演習環境のリアリティ, そして, 演習の振り返りを支援するサイバー演習統合管理システム “CABIN” を提案する. 本稿ではまず, 現状のサイバー演習との比較を経て, 演習環境の構築とリアリティ, そして振り返りを実現する機能について検討する. 次に CABIN の機能について概念実装と実装実験を行い, 課題の洗い出を行う. 最後に, 課題の整理とともに CABIN による新しいサイバー演習環境について考察を行う.

SATOSHI OHTA[1]　SHINGO YASUDA[1]　TSUBASA YUMURA[1]　YUUKI TAKANO[1]

1. はじめに

サイバー演習の必要性が認知されてきている. サイバー演習は目的によって, セミナーやワークショップ, 机上演習など, いくつかの種類がある [1]. 本稿は, 模擬システムを用いた実践的なサイバー演習を対象とする. 情報セキュリティに対する積極的な行動を促す要因の 1 つとして諏訪ら [2] は, “セキュリティ知識を授けるよりもセキュリティスキルを授ける事が望ましい” としている. また符号化特殊性原理 [3] から, リアリティの高い環境での演習体験が現場での対応力の向上に繋がるため, サイバー演習環境でのリアリティは必須な要素である. 加えてサイバー演習の体験と反省を繰り返す作業は, スキル忘却への対策として重要である. さらに演習内容を反省するためには, 演習内容を振り返りながら, 評価が提示される必要がある. そのため, サイバー演習の参加者 (以降,“参加者”) の挙動や操作ノード等の観測情報と, その情報に対する評価がなければならない. 監視や観測の機能は, サイバー演習に共通して必要な機能といえる.

[1] 国立研究開発法人 情報通信研究機構
NICT

現在のサイバー演習では, サイバー演習毎に専門の担当が時間と手間をかけて環境を構築しており, リアリティや監視/観測についてもサイバー演習毎で異なるため, 参加者のスキルの習得度もサイバー演習によって様々である.

本稿では, サイバー演習に必要なリアリティを維持しながら監視/観測する統合サイバー演習環境 “CABIN” を提案する.

CABIN は雛型となるトポロジを利用したサイバー演習環境の構築をサポートする. リアリティの支援や監視/観測機能による評価支援, ロールバックにより, 主催者の運用の簡便化を実現する. これにより演習機会の増加を図ると共に, 情報セキュリティの人材育成に寄与する.

今回,CABIN の概念実装として, 典型的な中小企業のネットワークを持つサイバー演習環境を構築した. 詳細は本論で述べる.

2. サイバー演習環境の課題

サイバー演習には, いくつかの形式がある. 総務省による実践的サイバー防御演習 (CYDER) [4] は, ログ履歴から過去の出来事を解析するフォレンジックスの演習である. それに対して,Web Application Security Forum(WAS

Forum) [5] が開催する Hardening [6] は, e コマースの運用という実践的なテーマの元で, リアルタイムで発生する複数のインシデントを克服する. SECCON [7] は情報セキュリティのコンテストである. 競技としていくつか種目があるが, その中に, 自チームサーバーを守りながら相手チームサーバーの脆弱性を攻める “Attack and Defense” 方式のサイバー演習がある.

サイバー演習環境は演習構築のコストが高く, また, 参加者のスキル向上を図る環境として考えた場合, 共通する課題がいくつか挙げられる. ここではこれらの問題点について考える.

サイバー演習環境の準備には, 演習環境の設計, 構成要素ごとのインストール, そして脆弱性などの, サイバー演習に必要となるコンテンツの作り込みがある. CYDER のサイバー演習のシナリオは社内ネットワークでのインシデントであり,Hardening のシナリオは e コマース,SECCON は 1 つの競技形式である. サイバー演習の中のネットワークトポロジは現実社会を模擬した物が多い. そのため, 個々のネットワークトポロジは類似しており, 雛型のネットワークトポロジを検討しやすい. Attack and Defense は競技形式であるため, 競技形式の基本内容を雛型のネットワークトポロジとして構築できる. 雛型のネットワークトポロジに, サイバー演習の運用に必要となる周辺の機能を運用雛型として加えることにより, 演習環境の雛型となる,“雛型演習環境” を構築する. この雛型演習環境を提供する事により, 準備にかかるコストを抑えられる.

リアリティは, 過去の生活感を表現する静的リアリティと, 現在の生活感を表現する動的リアリティがある. 参加者にとっては, 静的リアリティとしては, ログインしたサーバーやクライアントで確認できるログファイルやドキュメントファイルがあり, 動的リアリティとしてはネットワークの観測時に確認できるパケット, サーバーでのセッション状態, クライアントでのメール着信がある. これらのリアリティは演習内容の本流のシナリオと関係のない場合もあるため, サイバー演習環境によって対応に差異がある. Hardening はリアルタイムで進行するため, ネットワークを流れるパケットやメールのやりとりはリアルそのものである. しかし,e コマースを利用する他の購買客の購買行動で発生する環境の変化 (ネットワークパケット) など, シナリオに無関係な部分については省略されている. 前述の CYDER や Hardening などのサイバー演習の例では用いられていないが, マルウェアを演習中に利用する際には, ハニーポット 判別機能に対するリアリティが必要である. これはマルウェアが, 今存在する環境が動的解析環境のハニーポット上なのかを判別する技術で, ハニーポット上であると判別されると, マルウェアは本来の挙動を示さなくなる. そのため, マルウェアを利用する場合には, マルウェアに対して十分なリアリティを提供しなければならない.

以上のように, リアリティへの配慮については一方ではサイバー演習毎に対応に差異があり, 一方のマルウェアのようにリアリティが動作条件として必須な場合がある. 必要なリアリティの提供を柔軟に支援する事で, サイバー演習環境の作成者は主目的の構築に集中できる.

サイバー演習環境の運用管理のため, ネットワークやサーバーのメモリリソース等, 利用状況が監視/観測されている. それに加えて Hardening では WEB サーバーのクローラーを用いたり, SECCON の Attack and Defense では, 攻撃と防御それぞれで加点している. チェックポイントの確認等, イベントシナリオのための監視もある. CYDER や Hardening は, 参加者同士のコミュニケーションや連携作業に重点を置いている. これはセキュリティ対策面では, 重要な要素の 1 つである. しかし, サイバー演習の目的には参加者のスキルアップもある. 開催者が目指す目標とは別に, 個人レベルでの評価があれば, 直近の目標としてスキルアップに繋がりやすくなる. そのため, 参加者の操作内容の監視/観測も必要である. 様々な監視/観測を支援する事により, 運用管理機能の構築を容易にし, 参加者の振り返りが可能になる.

これまで述べたサイバー演習は数十人規模のイベントであり, 演習は参加者に対して 1 回の実施で終了となる. 復習のために再演習を行いたい場合や演習環境に不具合が起きた場合など, ロールバックが必要になる. ロールバックを容易に行えれば, 演習環境内の構成要素が壊れるようなシナリオでも繰り返しての実施が可能になる. 開始時まで戻るロールバックは各サイバー演習で可能であるが, 運用コストがかかる. 標準的なロールバック機能を提供できれば, サイバー演習の運用時のコストが低減できる.

3. サイバー演習統合管理システム “CABIN”

CABIN は複数のノードとネットワークを複数の参加者に対して, 同時並行的にサイバー演習環境を提供する.

図 1 は CABIN の概観図である.

CABIN は複数の物理サーバーを 1 つの大きな仮想環境として, サイバー演習環境用にそれぞれリソースを提供する. 実線で区切られているのは独立している様子を表しており, 他のサイバー演習環境からの影響は受けない. 各主催者は, 提供されたリソース上でサイバー演習環境を構築する. 各主催者は,CABIN 上で提供されている雛型トポロジを用いてサイバー演習環境を構築できる. CABIN が提供するリアリティ支援機能や監視/観測機能は, 主催者の選択によって利用が可能である.

3.1 雛型環境の提供

初期コストを抑えるため, サイバー演習で多く用いられる要素の雛型を提供する. 典型的な雛型としては以下のものが挙げられる.

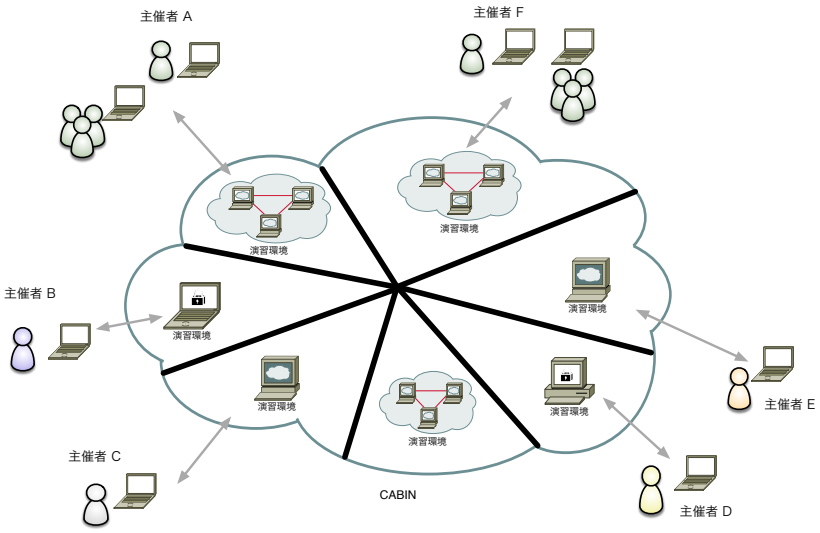

図 1　CABIN を使ったサイバー演習

- 演習運用インフラ：演習運用インフラは, 演習環境が必要とする, 外部とのインターフェースを提供する. 参加者が演習環境への接続をアシストする機能として “踏み台” がある. 踏み台は参加者の操作の起点となるため, 参加者が演じる役割によって, 担当用端末や攻撃用端末が用意される. その他, 演習環境の必要に応じてProxy,DNS,NTP,Mail サーバーを提供する. サーバーを提供する際には, 演習環境に接続するためのルーターの用意が必要である.
- 演習対象：演習環境を構成するノードであり, ネットワーク装置やクライアント, サーバーが提供される. WEB サーバー,Mail サーバー,DNS サーバーなどのサーバー類や, Windows や Linux クライアントなどの他, ルーター等のネットワーク機器も対象となる. また, 演習シナリオでは被害を受ける内容が多いことから, 脆弱性を持っている状態や汚染されている状態の端末やサーバーがあれば, 構築コストの低減に繋がる.
- 演習ネットワークトポロジ：演習環境のネットワークトポロジである. 中小企業の社内ネットワークを模擬としたトポロジはよく用いられる. サイバー演習の参加者の多くは企業が多いため, 一般的な企業ネットワークは雛型トポロジとして適している. 今後は参加者の増加により, トポロジも多様化すると考えられる.

これらの雛型を用いる事で, 簡単に多様なネットワークトポロジを持つサイバー演習環境を構築できる. サイバー演習環境は最新のセキュリティ技術動向に追従する必要があるため, 演習対象の雛型については, 新規情報を反映した雛型の提供を維持する必要がある.

3.2　リアリティ支援機能の提供

サイバー演習環境の外部からサイバー演習環境内部のサーバーへのアクセスや, メールサーバーへのメールの送付などを自動で行う機能があれば, ネットワーク内を流れるパケットを始めとした, WEB サーバーのログの更新やメール着信通知などの, ダイナミックな生活感が表現できる. これらは参加者の操作対象とならない外部要素であるため, CABIN が支援機能として標準的に提供する.

マルウェアは,C&C サーバーへのアクセス確認など, 外部ネットワークへの接続状態に基づく判断を行う場合がある. 挙動が解析されている既知のマルウェアであれば, 起動したマルウェアの情報とマルウェアから送出したパケット情報から, マルウェアが稼働するために必要な情報を応答する機能を提供する.

3.3　監視/観測機能の提供

監視/観測には,CABIN の運用管理を目的とする CABIN のリソース管理機能と, 参加者のスキルアップを目的とする参加者の挙動管理機能, そして, ロールバックのための演習状況の保存機能がある.

- CABIN のリソース管理機能
  CABIN 全体の運用のために保有リソースの空き状況や, 割当状況を管理する.
- 参加者の挙動管理機能
  反省の材料となる, 演習中の参加者の行動を記録する. 参加者が入力したキーの内容や操作コマンドの入力時刻などの挙動情報を収集するため, 演習運用インフラ内に, 参加者に関する情報を収集する機能を設ける.
- 演習状況の保存機能

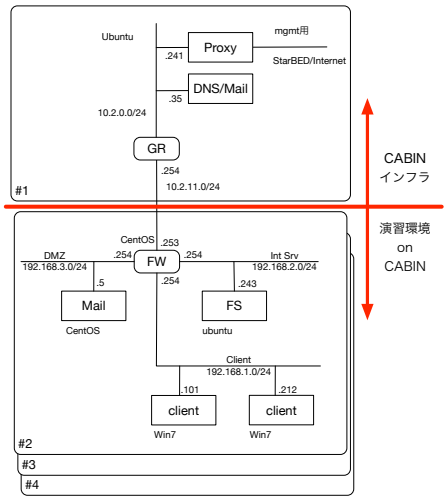

図 2 CABIN インフラと演習環境

演習状況は, 演習対象のサーバーやクライアントのログが必要である. 演習運用インフラからはメール送信や WEB アクセスなど, 演習対象への入力に相当する情報が得られるため, これら入力情報と, 演習対象内の応答内容の履歴が関連付けられる必要がある.

サイバー演習中の参加者の挙動や演習状況は, 主催者へのフィードバック情報として必要である. したがって, これらの監視/観測情報は, リアルタイムでの提供を可能とし, また, 演習終了後には速やかに収集されなければならない.

3.4 ロールバック機能の提供

サイバー演習において,“反省に基づく反復練習” はスキルアップとともにスキルの定着に必要である. また演習中に不具合が生じた場合, 演習環境を不具合発生前の状態へ容易に戻せられれば, 運用コストを抑えられる. 開始時点までのロールバックにより, 同一参加者の反復演習だけではなく, 複数参加者に対してスムーズな演習環境の提供が可能になる. また監視/観測機能による演習状況を活用する事により, 指定のチェックポイントへのロールバックが可能になる.

4. 概念実装

我々は 3 章で提案した CABIN の概念実装として, CABIN インフラとサイバー演習環境について次のように構築した.

図 2 は CABIN インフラと演習環境を示している.

サイバー演習環境は, 中小企業ネットワークを想定している. CABIN インフラ側は, サイバー演習環境へ接続するためのグローバルルータ “GR” と, メールサーバー “Mail”, そして, プロキシサーバー “Proxy” を設置した.

4.1 雛型演習環境の構築

今回中小企業の社内ネットワークを模擬したトポロジを雛型トポロジとして定義した. 1 台のファイアウォールにそれぞれ, DMZ ネットワーク, 社内サーバー用ネットワーク, そして, クライアント用ネットワークを用意する.

このトポロジには, 以下の要素を演習対象として構築することにした.

- ファイアーウォール：社内ネットワークの DMZ ネットワーク, 社内サーバー用ネットワーク, クライアント用ネットワークを接続し, ルーティングとファイアーウォール機能を持たせることとした.
- サーバー：社内に配置してある典型的なサーバーとして, メールサーバー, ファイルサーバー,DNS サーバーを用意する事とした.
- クライアント：事務で用いられている一般的なクライアントとして,Windows 端末を用意した.

演習運用インフラは, 演習環境に接続するルーター “GR” と, プロキシサーバー,DNS サーバー, メールサーバーを配置した. メールサーバーは後述のリアリティ支援を行っている. また, プロキシサーバーは管理用サーバーであり, 参加者からは利用できない.

これらの雛型を元にして, 環境構成図中の物理マシン#1 に演習運用インフラを,#2 内に演習環境の社内ネットワークを構築した. 図中の “FW” はファイアーウォール,“FS” はファイルサーバー,“Mail” はメールサーバーを示している. 環境の構築には Alfons [8] を用いており, 構築作業の効率を向上させている. Alfons を用いて, 物理マシン#2 の環境を, ホスト名や IP アドレス等の設定を変更しながら物理マシンの#3、#4 に配置した.

4.2 リアリティ支援

今回, リアリティ実現手法の 1 つとして外部メールサーバー内に自動送信機能を設けた. この自動送信機能は, 時刻の経過とともに演習環境内に向けてメールを送信する. 任意のメール内容を送付できるようになっており, 今回は実際に送られてきた一般的なメーリングリストの記事と共に, 演習シナリオに関係のある内容を混ぜて送信した.

4.3 監視/観測

今回の演習環境は参加者一人用であることから, クライアントにキーロガーを配置し, 参加者の挙動を記録することとした. 今回, サイバー演習主催者へのフィードバック部分については実装対象外としていたため, キーロガーによるロギング情報はクライアント内部に保存しておき, 演習終了後に回収した.

リアルタイムに回収する目的で, 監視/観測データを演習環境中のネットワークを利用事は, リアリティの欠如や演習そのものに影響を与える恐れがある. そのため, 監視/観

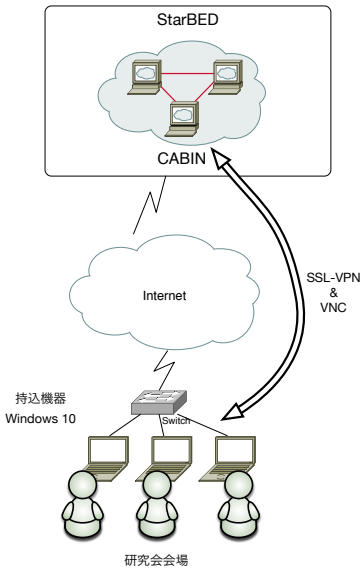

図 3 会場から CABIN への接続

測データリアルタイム取得専用のネットワークを用意するのが望ましい.

4.4 ロールバック

今回はより多くの参加者に体験してもらうため, ロールバックは演習開始時まで戻ることにし, 参加者が演習を終了する都度, 次の参加者に向けてロールバックする機能を実装した.

5. 実証実験

我々は 2015 年 9 月に第 1 回,2016 年 3 月に第 2 回として, WIDE 研究会で CABIN 概念実装モデル (以下,CABIN モデル) の技術課題の洗い出しを目的とした実験を行った. CABIN モデルによる演習環境は StarBED [9] に構築した.

CABIN へは図 3 に接続した.

会場会場に持参した各 Windows 端末に VPN と VNC ツールをインストールし, Windows 端末から図 2 の #2,#3,#4 へそれぞれ接続するようにした.

図 4 は会場での演習風景である. CABIN への接続用端末を卓上に配置し, 研究会の開催期間中は常に利用可能としていた.

5.1 実験の目的

第 1 回では, 構築した演習環境について操作感やリアリティについての確認を行い, 第 2 回では第 1 回からの改善点 (動的なリアリティや監視/観測) の効果の確認を行った.

5.2 サイバー演習内容

第 1 回, 第 2 回と, ともに実験参加者には攻撃者役として操作を依頼した. 演習の目的は, アカウントや特別権限など, 管理方法から生じる脆弱性について体験し, セキュリティを意識した運用管理の大切さを学ぶ.

「社内ネットワーク内のサーバーに用意された機密情報を取得する事が最終目標である」と伝え, 参加者本人の力で演習環境内を調べながら, 最終目標へ辿りつくシナリオになっている.

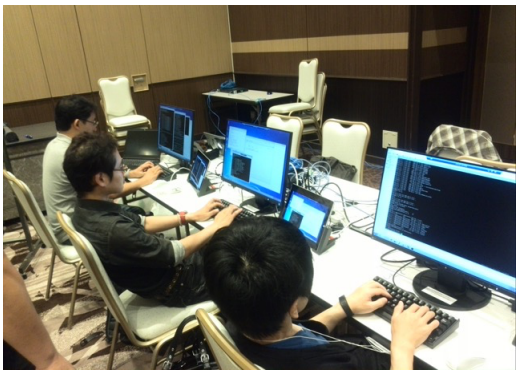

図 4 演習風景

5.3 結果

実験環境の構築と, 実験参加者への演習体験後のアンケートから, 次のような知見が得られた.

- 操作感
  リモートアクセスでもストレスなく操作が可能であった.
- 雛型環境
  第 1 回の演習環境の構築時に定義した中小企業ネットワークトポロジの雛型を, 第 2 回の演習環境の構築時に利用した. 第 1 回と第 2 回の演習環境では構成要素のクライアントとサーバーの数が異なっていたが, ネットワークトポロジの雛型は同じであったため,1 日で構築を終えられた.
- リアリティ支援
  第 1 回の実験で, 静的リアリティについての作り込み不足と, 動的リアリティへの配慮について指摘があった. 第 2 回の実験ではメールによる動的なリアリティを提供した.
  演習中に受信メールが増えている様子は好評であった. その一方で, 第 1 回実験の指摘からメール量を増やしたものの, まだ不足しているとの指摘を受けた.
- 監視/観測
  第 1 回の実験では, 各サーバー毎にキーロギングを行っていた. 各サーバーでの挙動に重点を置いていたが, 演習内容のふり返りには, 参加者の全ての挙動の情報が重要であることから, 第 2 回の実験では, 踏み台の Windows 端末上でキーロギングを行った. これにより, 参加者の全環境に対する操作情報を得られた.
- ロールバック

実験では, 新しい参加者向けに, 演習後の環境を開始状態に戻す目的で用いていた. 1 台のファイアウォール,2 台のサーバー (メール機能, ファイルサーバー機能), 2 台の Windows クライアントで構成される演習環境のロールバックは, 5 分の処理時間で可能であった.

6. 議論

6.1 課題

以下の内容について検討が必要である.

6.1.1 リアリティ

静的なリアリティについて, 次の課題がある.

- メール
  メールは社員 1 人あたり, 数百〜数千/月 のデータを処理していると考えた場合, クライアント側に相当量のメールが用意されていなければならない.
- 個人用フォルダやドキュメント
  ドキュメントの管理については, 個人用フォルダの内部は人によって管理方法が自由で異なるため, 個人用フォルダ内の階層などは個人差のある内容にしなければならない. また, 業務などで作成した個人のドキュメントも必要となる.
- 履歴
  クライアント上には,WEB ブラウザであればブックマークや閲覧履歴, 検索履歴などがあり, アプリケーションであれば「最近使ったファイル」など, 履歴情報を用意しなければならない. 一方でサーバーでは, 前述のメールサーバーのメールの着信履歴や,WEB サーバーのアクセス履歴など, サーバーが提供するサービスの利用履歴が必要である.

動的なリアリティについて, 次の課題がある.

- メール
  外部からのメール送付について今回, 時間経過による送付を可能にした.
- WEB
  WEB サーバーへのアクセスについては, 複数の模擬利用者によるアクセスを可能にする機能を現在検討中である [10]. 今後, 適用について検討する.

6.1.2 監視/観測

参加者のうち何人かは, 我々の用意した監視機能を発見していた. 演習環境として事前に説明をしてあったため停止や破壊はされなかったが, リアリティの観点からしても, 参加者が意識しない方法での監視/観測方法の検討が必要である.

今回キーロガーによる参加者の挙動情報を取得していた. これにより参加者の挙動については全て把握できるようになったが, 参加者の実施内容を振り返るためには, 参加者の行動の内容が十分であったかの判断が必要である.

例えば,「インシデント発生による調査依頼メールが送付されてきたため, 参加者は調査を実施する」シナリオにおいて参加者の行動を振り返るためには,

- 調査依頼メールの到着時間
- 参加者のメール確認時間
- 調査が必要とされているサーバーへのログイン時間
- 調査が必要とされているファイル等へのアクセス時間
- 対策が必要なコマンドの発行

の情報が必要となる. インシデントとその対応についていくつかシナリオのケースを用意し, そこで振り返りに必要となる情報をピックアップする事で監視/観測内に必要な情報や機能を検討する.

複数の参加者が参加する演習で振り返る場合には, 参加者個人の挙動の情報の他に, 参加者同士の共有情報の内容が必要となる. サイバー演習環境においてはメモなどの物理的なアイテムや,SNS などのアプリケーションかもしれない. 参加者間における情報共有の方法と内容の取得について検討が必要である.

6.1.3 ロールバック

研究会のデモンストレーションでは,3 つの演習環境をロールバックして使っていた. この参加者環境部分のロールバックには 5 分程度であった. 演習時間が短い場合には, 演習は開始地点からの繰り返しで十分であるが, 演習時間が長い場合や演習時間の短いシナリオを複数続けて演習した場合など, 復習したいポイントを演習開始時以外に設定を可能にすることにより, 効率良く再演習を行える.

演習開始時から参加者やサーバー, クライアントの全ての操作について監視/観測情報があり, 指定されたロールバックのポイントまで監視/観測情報に基づいて状態を変化させる事が可能であれば, 複数のロールバックポイントを再現できる.

6.2 資源の有効利用

今後は大規模なサイバー演習環境が必要とされている [11], [12]. 現在のサイバー演習環境では, 演習環境を構成するサーバーやクライアントの要素が全て稼働している. そのためサイバー演習環境の規模の最大値は, 利用可能な物理資源の規模の最大値で決定してしまう. スケーラビリティに欠ける物理リソースにおいて, 参加者が注目する部分の詳細化と, 非注目部分の機能の集約, 抽象化を組み合わせる事により, 物理的な資源の制約にとらわれないサイバー演習環境の構築を可能にする.

また同様に, サイバー演習の規模は小さいものの, サイバー演習による人材育成の機会の増加から, 演習の実施回数の増加が予想される. 1 台の物理マシン内で, 複数のサイバー演習を安全に隔離稼働させる技術を検討し, 同時並列的に稼働する数の規模の多い演習環境の構築を可能にする.

6.3 今後考えられるサイバー演習環境について

- サイバー演習環境のオンデマンド化
  現在のサイバー演習は主に, 国や企業での情報セキュリティに従事する人材の育成を目的とした, セキュリティリテラシーの高い層が対象となっている. しかし犯罪予防の点から考えると, サイバー犯罪の認識を目的とした, 情報リテラシーが低い一般ユーザー層に対するアプローチも必要である. 広い範囲でのサイバー演習の利用を考えた場合, セキュリティに詳しい演習環境の担当者がイベント毎に演習環境を構築から管理まで行う方法では対応が難しい. そのため, セキュリティの担当者が不在でも, 簡便, 安全, 安心に行える演習環境が必要となる.
- サイバー演習環境の相互接続
  高いセキュリティリテラシーを持つ, トップレベル層に対しても, スキルの維持を図れる環境について検討しなければいけない. この場合, トップレベル層に向けたサイバー演習環境を提供するのではなく, トップレベル層が構築したサイバー演習環境について, 相互接続と検証/評価を可能にすることにより, CABIN は切磋琢磨を図れる交流の場となる.

これらの実現に向けて, 独立利用する現状のサイバー演習環境とは別に, サイバー演習環境を公開利用する機能が必要となる. 公開利用では, 初心者向けの体験演習環境や, 攻撃用演習環境や防衛用演習環境などの, 異なる演習環境の相互接続を可能にする. 演習環境の利用目的や内容を多様化し, これらを通してサイバー演習環境も多様化させる.

7. おわりに

サイバー演習の目的の 1 つである, セキュリティスキルの向上に必要な要素は, 演習環境のリアリティと, 反復演習と反省を可能にする監視/観測機能である. CABIN はこれらを実現すると共に, サイバー演習環境の構築をサポートするサイバー演習統合管理システムである. 本稿では,CABIN の機能の定義と概念実装を行い, 過去 2 度に渡る実証実験について述べ, 結果と今後の課題について述べた. 今後は CABIN の各機能の実現と, 各課題について研究開発を行う.

参考文献

[1] 技術研究組合制御システムセキュリティセンター (CSSC),“サイバーセキュリティ演習”, 入手先 ⟨http://www.css-center.or.jp/pdf/cybersecurity-exercises_outline.pdf⟩ (参照 2016-05-05).

[2] 諏訪, 博彦 and 原, 賢 and 関, 良明, “情報セキュリティ行動モデルの構築—人はなぜセキュリティ行動をしないのか”, 情報処理学会論文誌,2012 年 vol.53,9 月,page:2204–2212.

[3] GODDEN, D. R. and BADDELEY, A. D. (1975), “CONTEXT-DEPENDENT MEMORY IN TWO NATURAL ENVIRONMENTS: ON LAND AND UNDERWATER”, British Journal of Psychology, 66:325-331,doi: 10.1111/j.2044-8295.1975.tb01468.x.

[4] 総務省: 実践的サイバー防御演習「CYDER」, 入手先 ⟨http://www.nisc.go.jp/conference/seisaku/jinzai/dai12/pdf/shiryou (参照 2016-05-05).

[5] Web Application Security Forum - WASForum, 入手先 ⟨http://wasforum.jp⟩ (参照 2016-05-05).

[6] Hardening Project 2016, 入手先 ⟨http://wasforum.jp/hardening-project/⟩ (参照 2016-05-05).

[7] SECCON:SECURITY CONTEST 入手先 ⟨http://2015.seccon.jp/⟩ (参照 2016-05-05).

[8] ビルディングブロック型模擬環境構築システム, S.Yasuda, R.Miura, S.Ohta Y.Takano T.Miyachi, インターネットコンファレンス (IC2015).

[9] 世界最大規模のエミュレーション基板 StarBED, 入手先 ⟨http://starbed.nict.go.jp⟩ (参照 2016-05-08)

[10] 湯村翼, “Sims in Cyber-Range”, 入手先 ⟨http://starbed.nict.go.jp/archives/starbed3/example/pdf/P-19.pdf⟩ (参照 2016-05-08)

[11] 内閣サイバーセキュリティセンター, 入手先 ⟨http://www.nisc.go.jp/index.html⟩ (参照 2016-05-05).

[12] サイバーセキュリティ戦略, 入手先 ⟨http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf⟩ (参照 2016-05-05).